

**ROUTING IN A DATA COMMUNICATION NETWORK****Field of the Invention**

5 This invention relates to data flow in communication and computer networks. The invention is applicable to, but not limited to, an addressing/routing mechanism for mobile nodes within such networks.

**10 Background of the Invention**

The Internet is becoming more and more popular, with access to the Internet being provided via computer networks and communication networks. The standard  
15 communication mechanism that communication units use to access the Internet is the well-known Internet Protocol (IP) version 4 and version 6.

Indeed, users increasingly wish to access the Internet  
20 whilst on the move via their mobile communication device(s). These devices are termed mobile nodes in IP-parlance. Different types of mobile nodes may be employed for this purpose, for example, a portable personal computer (PC), a mobile telephone or a personal  
25 digital assistant (PDA) with wireless communication capability. Furthermore, mobile users are accessing the Internet via different types of fixed or wireless access networks, for example a cellular radio communication network, such as a Universal Mobile Telecommunication  
30 System (UMTS) network, a HiperLAN/2 or IEEE 802.11b local area network, a Bluetooth™ local communication system, or fixed accesses such as the Ethernet, and so on.

It is currently possible to support handover accessing of the Internet from one access network to another, for example by using a protocol known as Mobile-IP.

Traditional mobility support aims to provide continuous  
5 Internet connectivity to mobile hosts, thereby allowing individual mobile users to connect to the Internet whilst being mobile by providing the mobile host with the opportunity to move the location of their Internet access. Recently, there has been a significant amount of  
10 interest and research in the Mobile IPv6 specification, as described in the document co-authored by David B. Johnson: IETF Internet-Draft draft-ietf-mobileip-ipv6-18.txt, June 2002.

15 Within IPv6 networks, host devices and client devices are allocated addresses comprising a hundred and twenty-eight bits to identify the device to other devices within, or external to, the network. The one hundred and twenty-eight bit addresses are known as Internet Protocol  
20 version 6 Addresses (IPv6 addresses). In the following, the terms IPv6 addresses and IP addresses are used interchangeably. IP addresses provide a simple mechanism for identifying the source and destination of messages sent within IP networks.

25 Traditionally, IP addresses that identify devices within IP networks have been assigned in a static manner during network configuration. Using this type of static assignment, data routers and other network components are  
30 pre-configured to use the statically assigned address bindings that correlate devices to their IP addresses.

However, in large or rapidly changing networks, static assignment of IP addresses is often inadequate. As a

result, several methods have been developed that allow IP addresses to be automatically assigned. The two widely used methods include:

- 5           (i) Automatic distribution by central servers, and
- (ii) Address derivation by a close cooperation
- between hosts and the immediately neighbouring router.

In another method employed in some IP networks, routers  
10 analyse IP data packets received from client devices. Every data packet has a source address and a destination address. The source addresses in these data packets are extracted and used to update routes within the router to deliver data packets to and/or from particular devices.  
15 In those latter types of networks routes are updated based on the packets circulating within the network, but addresses are not automatically assigned.

A tunnelled packet is a data packet that encapsulates  
20 within it another data packet. Thus, the encapsulating data packet has a pair of source and destination addresses. A further encapsulated packet has additional source and destination addresses, and so on. Such a tunnelling mechanism allows a Home Agent to keep track of  
25 the current position of a Mobile Node and forward packets from the home position (designated by an IP address, or Home Address) to the new position (a new IP address, or the Care-of Address). From a routing perspective, tunnelling allows a route of the data packet to be  
30 determined, e.g. by de-tunnelling the data packets to determine the source address of each encapsulated packet.

Increasingly, IP addresses within networks are assigned by server systems using the Dynamic Host Configuration

Protocol (DHCP) as is defined in Internet RFC 1541, which is incorporated herein by reference. For networks that use the DHCP protocol, one or more DHCP servers are configured to listen for messages requesting IP  
5 addresses. If possible, the DHCP server then allocates an IP address to the client system that sent the message. The newly allocated IP address is then included in a message sent by the DHCP server to the client system. The IP address is, in effect, provided to the client  
10 system on a time-limited basis, thereby allowing reuse of the same addresses by the same or a different client.

In general, the use of DHCP servers to assign IP addresses to client systems has proven to be particularly  
15 advantageous, saving non-expert users from manipulating long strings of digits (IP addresses). Furthermore, it allows an administrator tight control over the management of the address pool and guarantees the uniqueness of each used address. This is especially true in networks that  
20 include a large number of client systems.

Referring now to FIG. 1, a known IP routing mechanism is described that employs the IETF Mobile IPv6 protocol in a network. As an example, a network that is frequently  
25 found in a campus-type mobility network is shown. The network uses link technologies such as Ethernet and 802.11b.

In this regard, a mobile node 160 is operating in a  
30 micro-mobility (local-mobility) computer/ communication domain. The micro-mobility computer/ communication domain is configured as a tree structure, with a gateway 120 between nodes in the local domain and, say, the Internet 110. For example, let us assume the mobile node

is a portable computer that is able to communicate with the Internet 110 by wirelessly coupling to any of a number of access points/access routers 140-150.

5 The access routers are typically coupled to Dynamic Host Configuration Protocol (DHCP) Relays. The routing functionalities (in software) and the DHCP Relay functionalities (in software) are executed within the same access node. Optionally, the two functionalities  
10 can be spread over two different nodes, but with the restrictions that:

(i) The Relay must be placed on the link immediately next to the mobile node in order to receive  
15 the broadcasted address autoconfiguration messages sent by the mobile node, and

(ii) The Router functionality must be placed as far as possible towards the edge of the local mobility domain in order to ensure correct propagation of routes.

20

The micro-mobility domain includes routers 130, 132, 134 to link the access routers/DCHCP relays 140-150 to the gateway that includes a DHCP server 120. When the mobile node 160 has logged on to access router 140, it is  
25 assigned a temporary IP address, which is informed 165 to the MN's Home Agent 105. The MN 160 is able to access applications from application server 115, via a route 170 that encompasses the Internet 110, the gateway/DHCP server 120, and a number of serially-coupled intermediate  
30 routers 130 (with only one router shown) and the access router 140.

Notably, when the MN 160 logs on to another access router/DHCP relay 150, a new IP address is allocated to

the MN. The new IP address is informed in message 175 to the MN's Home Agent 105 so that communication towards the home position (home address) of the MN can be routed to the new position of the MN 160 (Care-of Address). In this regard, a skilled artisan would appreciate that a network that employs an IETF Mobile IPv6 protocol is not ideally suited for managing a micro-mobility (or local mobility) domain. The unsuitability emanates from a high control overhead resulting from frequent notifications to the Home Agent 105.

Methods that use DHCP and Mobile IP to manage mobility at an IP level are described in the documents by Charles E. Perkins, et al.:

- (i) "Using DHCP with Computers that Move", Proceedings of the Ninth Annual IEEE Workshop on Computer Communications, 1994; and
- (ii) "DHCP for Mobile Networking with TCP/IP", Proceedings of the IEEE Symposium on Computers and Communications, 1995.

DHCP is used to dynamically obtain a Care-of-Address (CoA) that will subsequently be registered with a Home Agent. In this manner, a Home Agent builds and maintains IP tunnels that deliver packets to mobile nodes through the routers 130, 132, 134.

A significant problem with mobile nodes is the requirement to assign new CoAs as and when the mobile node accesses the network via a different access point. Furthermore, the tunnelling requirement in such IP systems, particularly in a micro-mobility domain, has been appreciated by the inventors of the present invention as a further significant disadvantage.

US005812819A, titled "Remote Access Apparatus and Method  
which Allow Dynamic Internet Protocol (IP) Address  
Management", describes a mechanism to use the same CoA  
5 whilst changing points of attachment. The primary focus  
of US005812819A is to use a unique personal identifier,  
such that with each re-connection, a user obtains the  
same CoA. However, although US005812819A describes the  
maintenance of the same CoA, the mechanism still  
10 requires, and therefore suffers from the disadvantages  
of, inter-domain tunnelling by a Home Agent of Mobile  
IPv6.

'Address auto-configuration protocols' have been  
15 identified as an important requirement for IP mobile  
nodes in the following documents:

- (i) Dynamic Host Configuration Protocol for IPv6  
(DHCPv6), Internet Draft, draft-ietf-dhc-dhcpv6-19.txt;  
and
- 20 (ii) "DHCP for IPv6" by Charles E. Perkins, et al.  
Bound, and published at the Third IEEE Symposium on  
Computer and Communications, 1998.

The reasons identified for address auto-configuration  
25 protocols being an important requirement for IP mobile  
nodes include:

- (a) Due to the wide Internet penetration having  
led to the Transport Control Protocol (TCP)/IP stack to  
be deployed in general-purpose computing machines, the  
30 user of such a machine rarely has the skill (or the  
desire) to manually configure its TCP/IP stack.
- (b) With the advent of smaller and ubiquitous  
devices, it is often the case that there is no user to

configure the device stacks: they must be configured as Plug-n-Play.

In IPv6 there exist two address autoconfiguration mechanisms: 'stateless' and 'stateful'. The important difference between these two mechanisms is that stateful autoconfiguration uses a pair of hosts (server and relay) to maintain an address database as well as to relay a node's request and relay replies in the allocation of an address across a network. In stateless autoconfiguration the message exchange for autoconfiguration is limited to one link and there is no state to maintain.

WO9826549, titled "Method for Using DHCP to Override Learned IP Addresses in a Network", describes a method whereby DHCP messages are scanned for IP assignment events. When an event is triggered, a pre-configured IP route is updated in a central 'router' table.

Each route provides a mapping between an IP address and a client system. When the router receives an IP packet, it extracts the destination address of the packet from the packet's header. The router then searches the route table for a route that matches the destination address of the received IP packet. If the router finds a matching route, the router forwards the IP packet to the client system included in the matching route.

Notably, the method is applicable in a dialup environment, where all clients connect to one router and all accessed servers are situated directly connected on the same router. Hence, the applicability of WO9826549 is very limited.



Using the DHCP protocol, client systems request and receive dynamically allocated IP addresses from the DHCP server systems. The router listens for DHCP ACK messages sent by DHCP server systems to the client systems. The  
5 DHCP ACK message includes an IP address that has been allocated to a specific client system. When the router detects a DHCP ACK message, the router extracts the IP address allocated for the client system. Using the IP address included in the DHCP ACK message, the router  
10 "learns" the IP address of the client system requesting an IP address. The router then adds the route to its route table. The new route is marked to indicate that the DHCP server has assigned it. Thereafter, the router will only relearn this IP address if it is reassigned by  
15 the DHCP server system.

In some cases, the learned IP address will conflict with a route originally configured within the router's route table. In these cases, the conflicting route is removed  
20 from the route table. In this way, WO9826549 allows routes that reflect dynamically allocated IP addresses to replace already configured routes. The inventors of the present invention have recognised and appreciated the limitations of this method in that it is only able to  
25 update routers with new IP routes and is inadequate to handle new IP routes in a network scenario.

Moreover, the method provides for updates within only one "central" router, where all clients and servers are  
30 connected and using it as a unique "central" node of communication. It is known that such star networks are not implementable for large systems with hundreds of clients and thousands of servers. The inventors of the present invention have recognised a need to provide for

route updates within an entire cloud of routers, where everything is connected in a mesh-like topology, scaling the number of routes to connect any number of clients and servers.

5

US6249523, titled "Router for which a Logical Network Address which is not Unique to the Gateway Address in Default Routing Table Entries", presents a method to update ARP cache entries, effectively "routing" in a local broadcast link only, when triggered by DHCP messages.

It is noteworthy that the document titled "Cellular IPv6, Internet Draft Personal Proposal", draft-shelby-seamoby-cellular-ipv6-00.txt. describes a mechanism to manage IP mobility within a domain by appropriately updating per-host IP routes. Cellular IPv6 is a new protocol, which has been pending standardization for a number of years. Cellular IPv6 is equivalent to other routing protocols such as RIP. One of the reasons that Cellular IP has yet to be accepted for standardization is its use of paging concepts, which are natural in a 3GPP environment. However, such concepts are unfeasible with IP protocols, due to architectural inefficiencies such as network flooding (broadcast) of periodic (time-triggered) data over a large number of networks. Furthermore, the route status in this document is limited to a "personal proposal". As such, the mechanism is inadequate for standard IP mobility scenarios.

30

In summary, the inventors of the present invention have recognised that present implementations of IPv6 suffer from the need to regularly signal to remote home agents when a mobile node is mobile, for example, continuous

updating of the mobile node's CoA. Furthermore, IPv6 introduces problems in tunnelling requirements, when some configurations may not necessarily need to incur such complex and bandwidth/throughput costly mechanisms.

- 5 Current attempts at resolving one or more of the above problems have a consequent effect on other IP protocols.

#### **Statement of Invention**

- 10 In accordance with a first aspect of the present invention, there is provided a method of supporting mobility in an Internet Protocol (IP)-based data network, as claimed in Claim 1.

- 15 In accordance with a second aspect of the present invention, there is provided an access node such as a DHCP Relay, as claimed in Claim 7.

- In accordance with a third aspect of the present  
20 invention, there is provided a DHCP Server, as claimed in Claim 8.

- In accordance with a fourth aspect of the present  
invention, there is provided a data communication  
25 network, as claimed in Claim 14.

- In accordance with a fifth aspect of the present  
invention, there is provided an IPv6 communication  
message, as claimed in Claim 18.

- 30 In accordance with a sixth aspect of the present invention, there is provided a storage medium, as claimed in Claim 19.

In accordance with a seventh aspect of the present invention, there is provided an apparatus, as claimed in Claim 20.

- 5 In accordance with an eighth aspect of the present invention, there is provided a communication unit, as claimed in Claim 21.

- 10 In accordance with a ninth aspect of the present invention, there is provided a data communication network, as claimed in Claim 22.

Further aspects of the present invention are as claimed in the dependent Claims.

15

- In summary, the preferred embodiment of the present invention describes a mechanism to manage IPv6 local mobility without requiring any tunnelling of data messages towards a remote Home Agent. The mechanism  
20 utilises address autoconfiguration mechanisms capable of use in route maintenance. Advantageously, route update messages may be sent from both a DHCP Server and an access node such as a DHCP Relay when new IP routes are determined. Preferably, old or unacceptable IP routes  
25 are deleted within the local mobility. The method is able to use standard IETF protocols, such as DHCPv6 and RIP.

#### **Brief Description of the Drawings**

30

FIG. 1 illustrates a known computer/communication mobile network and mechanism for communicating to a mobile node.

Exemplary embodiments of the present invention will now be described, with reference to the accompanying drawings, in which:

5 FIG. 2 illustrates a computer/communication mobile network adapted to implement the preferred embodiment of the present invention;

FIG. 3 illustrates a Dynamic Host Configuration Protocol  
10 (DHCP) Server adapted to implement the preferred embodiment of the present invention;

FIG. 4 illustrates a flowchart of a process implemented by an access router DHCP Relay according to the preferred  
15 embodiment of the present invention; and

FIG. 5 illustrates a flowchart of a process implemented by a DHCP server, according to the preferred embodiment of the present invention.  
20

#### **Description of Preferred Embodiments**

Referring now to FIG. 2, a network configuration is  
25 illustrated in accordance with the preferred embodiment of the present invention. The network configuration preferably employs the IETF Mobile IPv6 protocol. As an example, a network that is frequently found in a campus-type mobility network is shown. The network uses link  
30 technologies such as Ethernet and 802.11b.

The preferred network topology, as illustrated in FIG. 2, is a tree-type structure as known to those skilled in the art. However, although the preferred embodiment is

described with reference to a tree-type structure, the inventive concepts described herein are equally applicable to any mesh-type structure. Conceptually, the root of the tree corresponds to the DHCP server (DS),  
5 with the MN movement managed only by the leaves of the tree. The preferred embodiment shows the last hops as using wireless access media, to communicate to the mobile nodes, although any access mechanism is acceptable (including dialup and other wired accesses like DSL, or  
10 plain Ethernet).

It is also assumed, in the context of the preferred embodiment of the present invention, that each access router (AR) is co-located with a DHCP relay (DR), and the  
15 Internet Gateway with the DHCPv6 Server respectively. All intermediate routers are normal routers.

In this regard, a mobile node 160 is operating in a micro-mobility (local) computer/communication domain.  
20 The micro-mobility (local) computer/communication domain is configured as a tree structure, with a gateway 220 between nodes in the local domain and, say, the Internet 110. For example, let us assume the mobile node is a portable computer that is able to communicate with the  
25 Internet 110 by wirelessly coupling to any of a number of access points/access routers 240-250.

The micro-mobility domain includes routers 230, 232, 234 linking the access routers/DCHCP relays 240-250 to the  
30 gateway that includes a DHCP server 220. When the mobile node 160 has logged on to access router 240, it is assigned a temporary IP address, which is informed 165 to the MN's Home Agent 105. The MN 160 is able to access applications from application server 115, via a route 170

that encompassed the Internet 210, the gateway/DHCP server 220, and a number of arbitrarily, or mesh-coupled intermediate routers 230 (with any number of intermediate routers on each path shown) and the access router 240.

5

Notably, in accordance with the preferred embodiment of the present invention, when the MN 160 logs on to another access router/DHCP relay 250, the same IP address is used. In this regard, when a MN changes its point of  
10 attachment between two Access Routers (AR), say AR 240 and AR 250, it confirms its previously acquired address to the DHCPv6 Server (DS) 220 via the DHCPv6 Relay (DR) co-located with the current AR 250. A 'CONFIRM' message then triggers an updating of routes in the DS 220, from  
15 the path towards the previous AR 240, to the path towards the new AR 250 with the route including all of the corresponding intermediate routers 234. A new route is therefore added to the address within the message by the access router/DHCP relay 250. The 'CONFIRM' message is  
20 concurrently relayed to the DS 220.

Instead of passing on a potentially new CoA for the new route to the Home Agent 105 of the MN 160, the DS 220 effectively receives the 'CONFIRM' message from the DR  
25 containing the same CoA (the "confirmed" address) and updates its routing table. In this manner, any new messages for MN 160, coming from the Internet 110 and sent via the gateway/DHCP server 220 are intercepted and re-routed to the new address, thereby not following the  
30 old route.

Thus, it is envisaged that any access node, for example a dynamic host configuration protocol (DHCP) Relay 250 includes a receiving function receiving at least one

Internet Protocol (IP) message from a mobile node,  
wherein the IP message includes a mobile node address  
capable of use for route maintenance to deliver data to  
and/or from the mobile node. The access node also  
5 includes a processor, operably coupled to the receiving  
function, to intercept and analyse the IP message, and  
determine a route to deliver data to and/or from the  
mobile node. The access node 250 triggers a transmission  
of one or more route update messages from via a number of  
10 network elements (such as intermediate routers 230  
between said access node to a DHCP server in the IP based  
data network.

Preferably, the old route is deleted; once the  
15 gateway/DHCP server 220 has accepted the new route to the  
MN 160, in order to correctly forward packets coming from  
inside the local-mobility domain.

The networking protocols are based on IPv6 and as such  
20 employ IPv6 stateful address autoconfiguration (i.e.  
DHCPv6) and a distance-vector routing protocol. A  
preferred distance-vector routing protocol, such as  
Triggered Routing Information Protocol (RIP), is used.  
In this regard, the DHCP CONFIRM message is used to  
25 trigger the Triggered RIP.

#### Autoconfiguration:

A stateful autoconfiguration mechanism is selected as the  
30 presence of a DR and DS 220 at the extremities of the  
micro-mobility routing domain allows tight control of  
routing path updates. In the stateless case, the routing  
path update(s) can only be triggered by one end of the  
routing path, i.e. the AR 250.



A particular message exchange deals with the renewal (or release thereof) of an already allocated IPv6 address of an MN when this moves to a new link. The message  
5 exchange tracks the following process: upon detection of movement and after attaching to a new AR 250, the MN 160 generates a CONFIRM message containing various identifiers of its configured interfaces, among which it uses the address it had used when first configuring this  
10 interface with a server. The CONFIRM message is sent to the DR (supposedly co-located with the new AR) and next propagated to the DS 220. Following reception of the 'CONFIRM' message, the DS 220 generates a 'REPLY' message to send to the MN 160 through the corresponding DR. In  
15 this way, the DHCPv6 transaction is completed and the MN 160 can continue to use the originally allocated address within the new subnet under the new AR 250.

Triggering Mechanism:

20 The preferred triggering mechanism is a set of processor-implementable instructions (i.e. software) that couples the interpretation of DHCP messages (CONFIRM by DS and DR and ACK for DR) with RIP messages (Unsolicited Route  
25 Updates). The reception and interpretation of standard DHCP messages is enhanced to launch standard RIP messages. Routing Information Protocol (RIP) is a standard distance-vector algorithm for exchanging routing  
30 messages and computing routes within an Administrative Domain.

The preferred embodiment of the present invention is independent of the underlying per-host routing protocol,

and employs a slight modification of RIP such that the protocol:

- (i) Includes standard RIP v2 features;
- 5       (ii) Includes standard Triggered RIP extensions;
- (iii) Includes standard RIPv6 extensions, since  
this is an IPv6 environment;
- (iv) Provides periodic updates by transmitting  
entire routing tables are entirely removed; and
- 10       (v) Propagates updates of per-host routes upon  
reception of Triggered update.

Traditionally, IP routing protocols are designed with no specific topology assumptions. In such circumstances,  
15 the underlying model assumes that the connectivity among routers takes the form of, say, a graph and links periodically fail and come up. A routing protocol is designed such that the network as a whole survives this kind of interruption.

20 In this manner, the network provides IP mobility within a local mobility domain by setting up and maintaining IP routes. When a MN changes its point of attachment between two Access Routers (AR) it confirms its  
25 previously acquired address to the DHCPv6 Server (DS) via the DHCPv6 Relay (DR) co-located with the current AR. The CONFIRM message triggers the launch of Triggered Route Updates, thus changing the routes in the DS, the previous AR, the new AR and in all intermediate routers.

30 A skilled artisan would recognise that the number of elements shown in the network of FIG. 2 are limited for clarity purposes only. Furthermore, it is within the contemplation of the invention that other network

configurations and inter-coupling of elements can be used.

Advantageously, the inventors of the present invention  
5 have recognised and appreciated the wider benefits  
offered by dynamically building and maintaining per-host  
routes within a small micro-mobility domain. In  
particular, the inventors have identified that per-host  
routing, which has traditionally been implemented for  
10 large-sized networks such as the Internet that spans  
continents and supports large-size of routing tables and  
very frequent updates of a large number of mobiles), is  
more appropriate than using tunnels due to the:

- 15 (i) Simplicity of routing protocols and wide  
availability of implementations;
- (ii) More efficient use of bandwidth, otherwise  
used to encapsulate packets in a tunnelling mechanism;
- (iii) Avoidance of a need to introduce entirely  
20 new protocol entities (local mobility agents); and
- (iv) Relatively minor adaptation of existing  
routers and DHCPv6 servers, as described below.

Hierarchical Mobile IPv6 schemes, as described by: Claude  
25 Castellucia, in "A Hierarchical Mobile IPv6 Proposal", of  
the 4<sup>th</sup> ACTS Mobile Communications Summit, 1999 and David  
B. Johnson and Charles E. Perkins in Hierarchical Foreign  
Agents and Regional Registration, Minutes of the Mobile  
IP working group meeting, 35<sup>th</sup> IETF, March 1996. The  
30 inventive concepts of the present invention provide two  
important benefits over known Hierarchical Mobile IPv6  
schemes:

- (i) Bandwidth savings by eliminating tunnels.

(ii) Elimination of local mobility management entities (e.g. MAP) that have been pending IETF standardization for several years.

(iii) Use of the same CoA within the entire  
5 local-mobility domain (HMIP changes the CoA, but does not propagate the change up to the distant home agent (HA). Advantageously, the inventive concepts described herein not only avoid propagating the CoA to HA, but maintain the same CoA).

10

When compared to all other micro-mobility (or local mobility) management schemes, the inventive concepts herein described provide:

15 (i) The inherent configuration flexibility of stateful autoconfiguration, whereas the other micro-mobility management schemes all suppose the IP address is manually configured;

(ii) Ability to implement a more rapid  
20 propagation of route updates by simultaneously triggering route updates from two separate points of the tree, namely the DS and the DR, whereas other micro-mobility management schemes trigger the route update from one point only; and

25 (iii) The process of the present invention is able to use standard IETF protocols.

Referring now to FIG. 3, a Dynamic Host Configuration Protocol (DHCP) Server 310 adapted in accordance with the  
30 preferred embodiment of the present invention, is illustrated. The DHCP Server 310 includes a signal processing function 320 operably coupled to a receiving function 325 and a memory element 330. The memory element comprises a router processing function 340 and a

route table 350. The DHCP Server 310 communicates to other devices in the network via an input port 360 and an output port 370. The DHCP Process uses a DHCP Address Table to keep track of assignments of addresses to  
5 mobiles, as well as approving and denying requests.

In accordance with the preferred embodiment of the present invention, the receiving function receives at least one first Internet Protocol message from a mobile  
10 node through a first access node, as described above. The at least one first Internet Protocol message comprises an address that is used to build a data route to deliver data to and/or from the mobile node via the first access node. The signal processing function 320  
15 processes the first Internet Protocol message to determine the data route to/from the mobile node, and stores the route information.

The DHCP Server 310 has been adapted to receive at least  
20 one second Internet Protocol message from the mobile node through a second access node, such that the second Internet Protocol message comprises an address used to build a second data route. The signal processing function 320 then determines whether the second data  
25 route is the same as the stored first data route. In response to the determination, the DHCP Server 310 triggers a message to all its neighbour routers and subsequently to all routers in the routing domain deleting the first data route if the second route is  
30 accepted. Alternatively, the DHCP Server 310 triggers a message to the second access node deleting the second data route, if the new route is not accepted.

Preferably, the first and second Internet Protocol messages are IPv6 messages such as IPv6 stateful autoconfiguration 'CONFIRM' messages. In an enhanced embodiment of the present invention, the signal  
5 processing function 320 intercepts DHCPv6 stateful autoconfiguration IP messages sent from mobile nodes via ARs and processes the message to determine a new data route to deliver data to and/or from the mobile node. In response, the new route is used to update the data route  
10 in the router table in response to the processed DHCPv6 stateful autoconfiguration IP message. The signal processing function 320 then sends a delete route message to network elements in the data route to update their route records.

15 Referring now to FIG. 4, a flowchart 400 illustrates a preferred operation of the Access Router. It is assumed that the MN has already configured an address for its interface with a normal DHCPv6 transaction, as described  
20 above with respect to FIG. 2. Furthermore, it is assumed that the MN is currently active within a sub-network, whilst its routing address indicates access to/from the MN via the old AR. The mobile node has previously confirmed this old address to the DS through the DR.

25 The operation of the new AR starts in step 410. The MN moves to a new AR. The MN generates a 'CONFIRM' message and transmits this message to the new AR as shown in step 420. Upon reception of the CONFIRM message in step 430,  
30 the AR memorises the interface address from which it received the 'CONFIRM' message, in step 440.

The DR (operably coupled to the AR) routes the 'CONFIRM' message up to the DS, as shown in step 450. In addition,

the DR also adds a new route to this address through the (memorised) interface address that received the 'CONFIRM' message, as in step 460. This route addition to the 'CONFIRM' message is propagated up-stream to all  
5 intermediary routers in the new path to the DS, preferably by means of Unsolicited Route Update messages, as shown in step 470. In this manner, the MN has moved to a new access point and a new route to the MN has been generated by the AR/DR in the 'CONFIRM' message sent to  
10 the DS.

Referring now to FIG. 5, a flowchart 500 illustrates a preferred operation of the DHCPv6 Server (DS), in response to receiving a 'CONFIRM' message with a new  
15 route update from the AR/DR as described above with respect to FIG. 4.

The DS operation starts in step 510. Upon reception of the 'CONFIRM' Relay-Forward message from the new AR in  
20 step 520, the DS decides to either reply positively (preferably triggering deletion of the old route) or negatively (preferably triggering deletion of the new route previously added by DR), in step 530.

25 It is envisaged that the DS replies negatively when it decides that the MN took too much time to switch between ARs. For example, the laptop MN may have entered a sleep mode, or even turned off, in which case the DS denies the CONFIRM because the address was allocated to another new  
30 MN in the meantime. Alternatively, when the MN connects to another local-mobility domain, it will CONFIRM this address towards another DHCP Server that doesn't own that address.

If the DS decides to reply negatively to the 'CONFIRM' message in step 530, the DS triggers propagation of a route deletion message to all intermediary routers to the new AR, in step 540. In this manner, all intermediary  
5 routers that have just recorded a new route to the MN address, as extracted from the 'CONFIRM' message sent from the AR to the DS, will delete the new route record. In this regard, the DS sends a reply to the 'CONFIRM' message to the MN, via the corresponding AR/DR, to inform  
10 the MN, and implicitly the intercepting AR/DR of the negative decision, as shown in step 550.

If the DS decides to reply positively to the 'CONFIRM' message in step 530, the DS removes the old route to the  
15 MN assigned address, as stored in its internal routing table as shown in step 560. Substantially concurrently, the DS adds the new route entry to the MN assigned address, where the route indicates the interface through which the 'CONFIRM' message was received, as in step 570.  
20 The DS then triggers propagation of a route deletion message to all intermediary routers between itself and the old AR/DR, in step 580. In this manner, all intermediary routers that have recorded a now obsolete route to the MN address will delete the route record. In  
25 this regard, the DS sends a reply to the 'CONFIRM' message to the MN, via the corresponding DR. The reply informs the MN, and implicitly the intercepting DR/AR of the negative decision, as shown in step 550.

30 In this manner, the DHCPv6 Server is able to allocate the same (CoA) address to the MN, upon the MN moving to a new access router. Advantageously, in this approach, the MN's care-of-address is then maintained as a valid address for the entire micro-mobility domain,



irrespective of which access router the MN uses within the domain.

Furthermore, by intercepting the message to the home  
5 network, the combination of the new AR/DR and DHCPv6  
Server is able to maintain an IP address to the MN,  
without taking up valuable bandwidth resource in  
propagating the new route within the micro-mobility  
domain to higher entities in the network.

10

A further advantage of this mechanism is that, by  
provision of a single MN CoA throughout the local  
mobility (micro-mobility) domain, there is no requirement  
to perform tunnelling and de-tunnelling operations, which  
15 also take up valuable resource (i.e. computing resource  
on nodes and bandwidth resource on networks).

The inventive concepts of the present invention find  
particular applicability in mobility-supporting network  
20 domains such as a university campus or in a company where  
nodes are, for example, spread over multiple-storeys in a  
building. The topology of such networks is typically a  
tree-structure with rarely more than three levels in the  
structure. The mobility population of such domains  
25 typically encompass a few hundred nodes. The majority of  
the communication in these domains takes place among  
nodes within the domain, and not to an external Internet.  
Furthermore, local nodes are able to move within the  
domain. Also, visiting nodes can be accepted to visit  
30 and move within this domain quite readily.

Such a domain preferably deploys an Interior Gateway  
Protocol (IGP) routing protocol, for example a Routing  
Information Protocol (RIP), as well as a stateful address

autoconfiguration scheme such as (DHCP). Thus, within this domain, it is more economically viable to reuse DHCP and RIP functionalities rather than deploying Mobile IP entities, which would require modifying every client PC, every server and introducing home agents.

The inventors of the present invention have recognised that in such a domain, the DHCP server (DS) is never in a situation to refuse a CONFIRM message. Hence, a moving PC will always use the same care-of-address within this domain. This address is its only address and there is therefore never a need to assign a Home Address and a Care-of-Address as is required by Mobile IPv6.

In this case, a modified operation of the AR/DR in FIG. 4, as well as the DS in FIG. 5, can be implemented. In particular, it is envisaged that both the DS and AR may trigger the route addition to all intermediate routers. Advantageously, such a two-pronged route update triggering mechanism effectively leads to faster updates.

Thus, a mechanism to combine address autoconfiguration with route maintenance, in order to support mobility, has been described. This is in contrast to traditional address autoconfiguration mechanisms, which have been performed entirely automatically and separately from route maintenance. Route maintenance has been performed in a half-manual/half automatic manner, inasmuch as routing information is initially introduced manually in each router and then routers communicate with each other to discover the shortest available routes.

It is to be appreciated that the arrangement and specific details of interfaces, address types, routers, etc. in

the above embodiments are merely examples, and the invention is not limited to these examples. The invention should be viewed as capable of being applied to other types of data (computer/communication) networks or protocols and subnets thereof. Furthermore, the invention may also be applied to domains other than a tree-structure or a substantially micro-mobility domain, when such networks have subnets and access networks whose functions correspond to those described above.

10

The invention, or at least embodiments thereof, tend to provide the following advantages, singly or in combination:

15

(i) A data packet may be transmitted much more efficiently, with a minimum of number of tunnelling operations performed by intermediary routers, thereby achieving improved route updating.

20

(ii) When compared to hierarchical Mobile IPv6 schemes, the inventive concepts described above provide:

(a) Bandwidth savings, by eliminating tunnels; and

(b) Elimination of local mobility management entities (e.g. Mobility Anchor Point (MAP)) which have been pending IETF standardization for several years.

(c) Use of the same CoA, avoids updating not only the distant HA but also any new entity, such as a MAP.

30

(iii) When compared to all other micro-mobility (or local mobility) management schemes, the inventive concepts described above provide:

(a) Inherent configuration flexibility of stateful autoconfiguration, in contrast to other micro-mobility management schemes where the IP address is manually configured;

5 (b) A more rapid propagation of route updates, by simultaneously triggering from two separate points of the tree, namely the DS and the DR; and

(c) Compatibility benefits as standard IETF protocols can be used.

10

(iv) When compared to Cellular IPv6, the present invention does not use any form of paging. Thus, no broadcasting of data is required and a more efficient and less bandwidth hungry solution is achieved. In contrast  
15 to Cellular IP, the present invention proposes a "per-host routes" proposal, that notably relies on standard RIP and DHCP as existing, fully specified, software available solutions.

20 (v) The technique benefits from using the same CoA for the routing of all data packets to a particular mobile node, say within a micro-mobility domain, but with the elimination of intra-domain tunnelling suffered by the mechanism proposed in US005812819A.

25

Whilst the specific and preferred implementations of the embodiments of the present invention are described above, it is clear that one skilled in the art could readily apply variations and modifications to the preferred  
30 embodiments that fall within the inventive concepts.

Thus, a methods to support local mobility in TCP/IP networks and associated network elements have been described, whereby the disadvantages associated with

known mechanisms, apparatus and methods have been substantially alleviated.